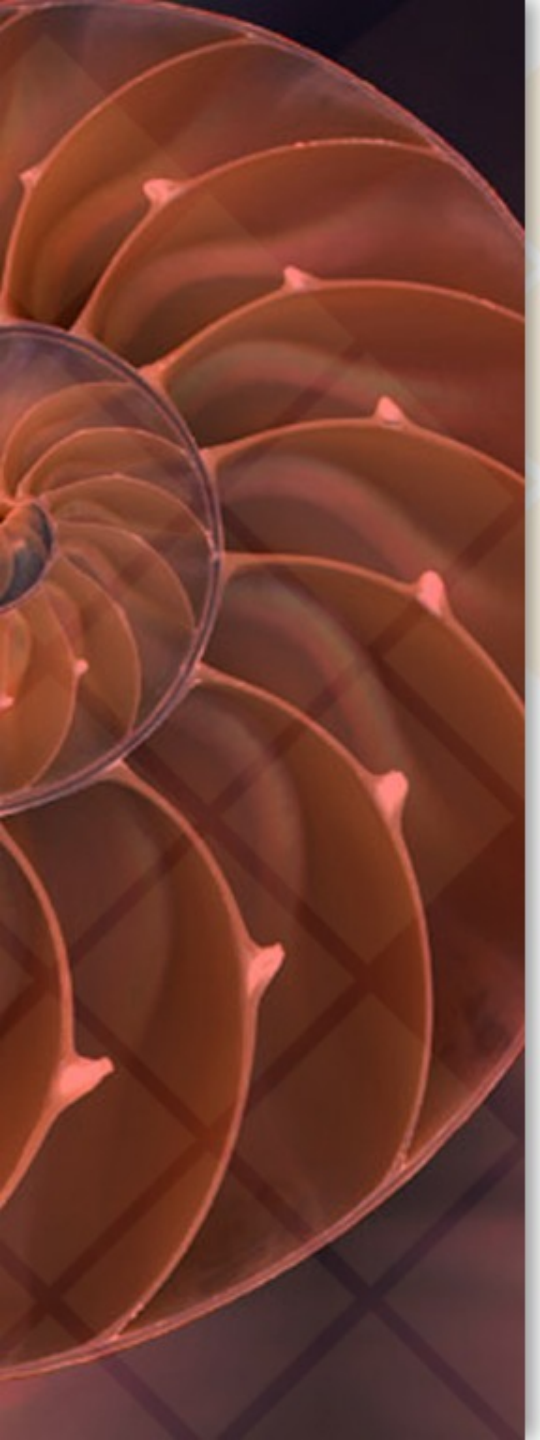


Graph Matching Technologies for Behavior Prediction

Culture and Adversary Modeling Workshop
November 29 – December 1, 2005
San Antonio, Texas

Tim Darr
21st Century Technologies

Mike Wellman
University of Michigan

Distribution A: Approved for public release; distribution unlimited.

Copyright © 2005, 21st Century Technologies. All Rights Reserved.
<>This document may not be copied or used in any way without the express written permission of 21st Century Technologies. The products described in this document are and shall remain the property of 21st Century Technologies. Terrorist Modus Operandi Discovery System (TMODS) is the trademark of 21st Century Technologies in the U.S. and other countries. All rights reserved.

Briefing Outline

- Game-Theoretic Terrorist Modus Operandi Detection System (GT-TMODS)
- Graph Pattern Matching
- Social Network Analysis
- GT-TMODS
  - Key Ideas
  - Contributions
  - Representation
  - Examples
- Question / Answer

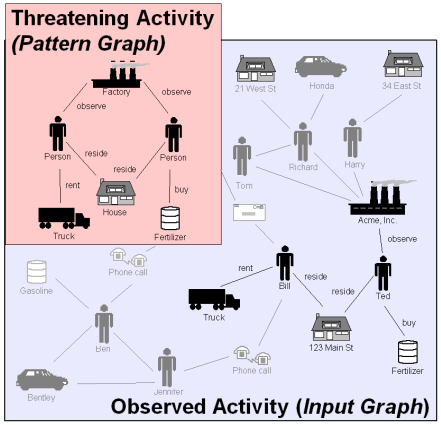
GT-TMODS

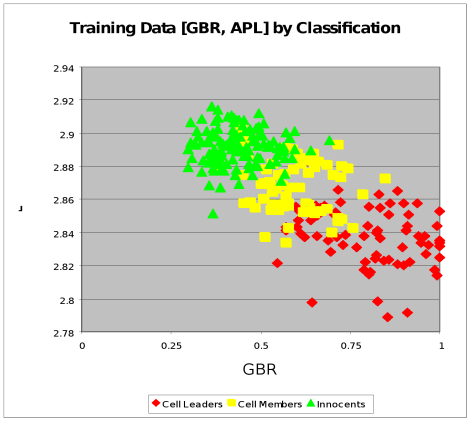
- GT-TMODS (Game-Theoretic Terrorist Modus Operandi Discovery System) is an integration of graph pattern matching, Social Network Analysis (SNA), and game-theoretic modeling
- Partners
  - Professor Mike Wellman
  - University of Michigan AI Lab

Problem Statement

Today's CT intelligence analysts face significant challenges

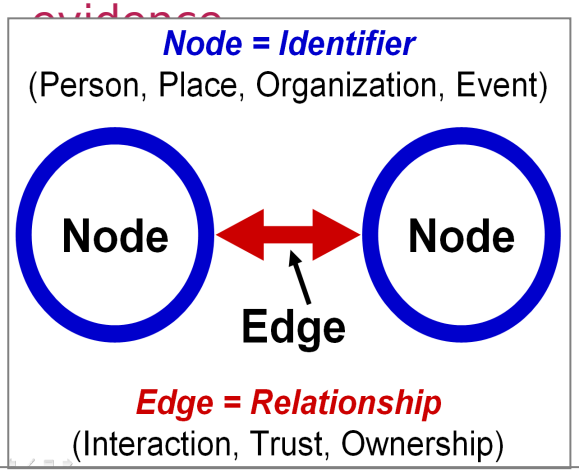
- TMODS applies our existing *graph matching* and *social network analysis* capabilities to the asymmetric threat detection problem
- Graph matching finds specific patterns in a network activity graph (suspicious financial transactions)
- Social network analysis (SNA) characterizes activity as normal or abnormal based on *metrics* computed on the activity graph





A New Approach to the Asymmetric Threat Detection Problem

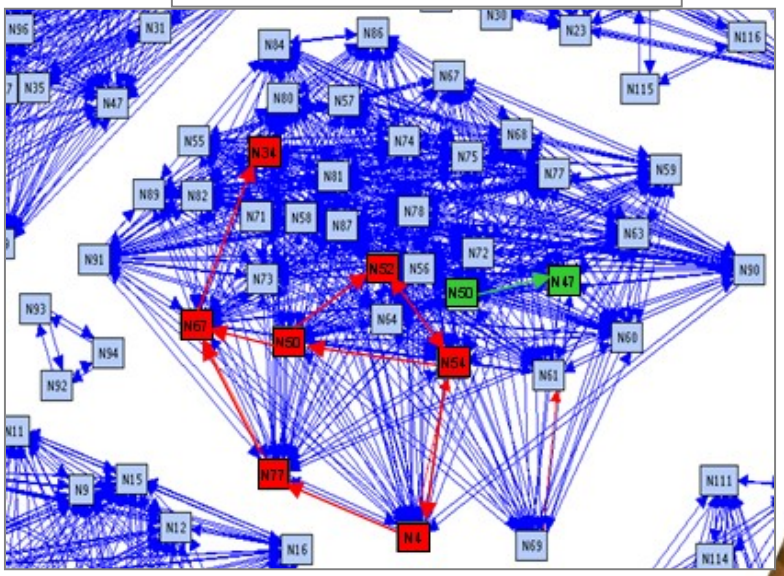
- Pattern recognition
  - Find threatening activity hidden in benign activity
- Information overload
  - Almost all activity is benign
  - Faint signal in lots of noise
- No ground truth available
  - Incomplete/inaccurate evidence



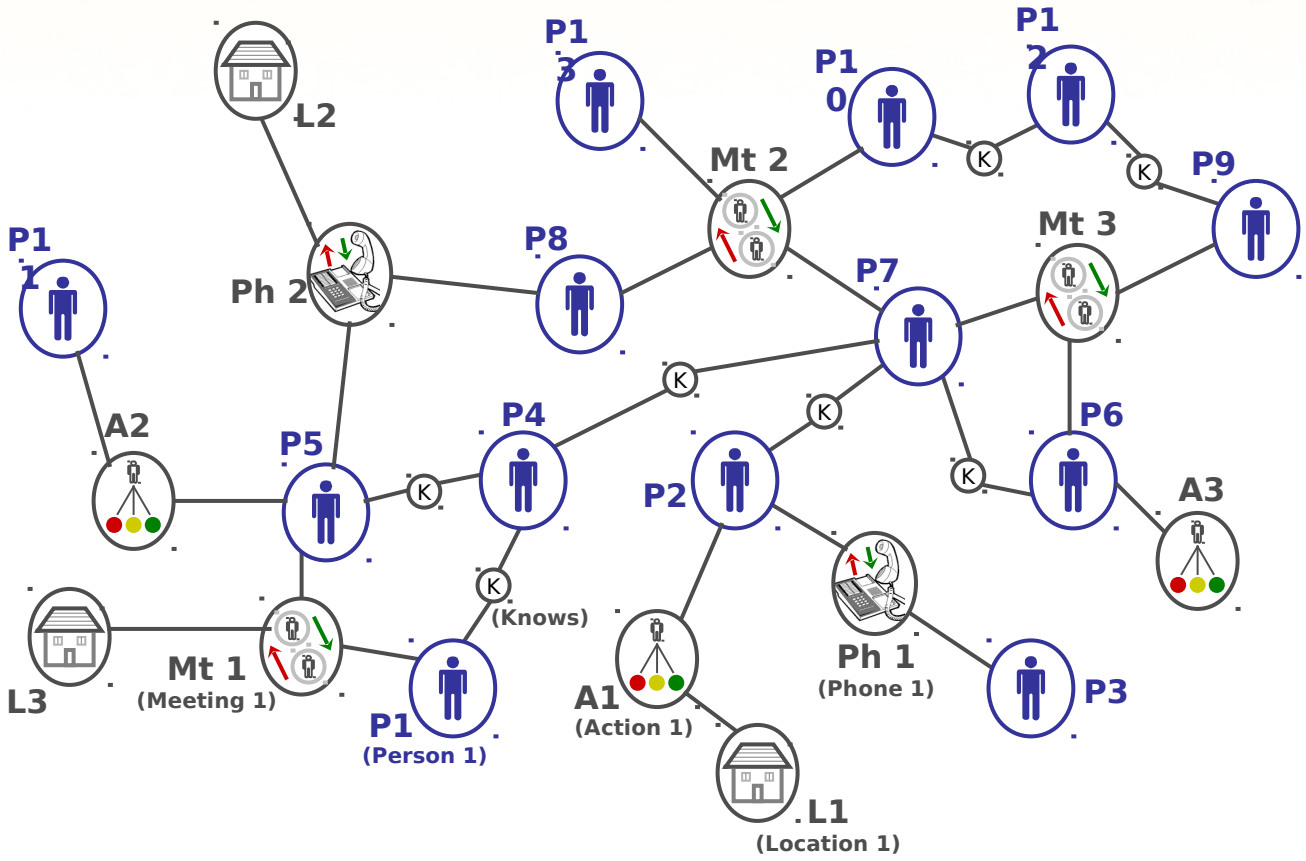
We model complex systems as a network of nodes and edges

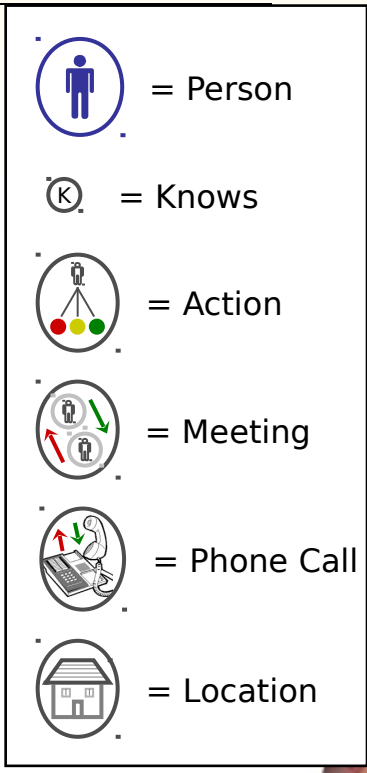
- Our solution: View the world as a graph
  - Natural visualization
  - Allows for combined attribute and structure searches
  - Tolerant of noise

Sample Activity Graph

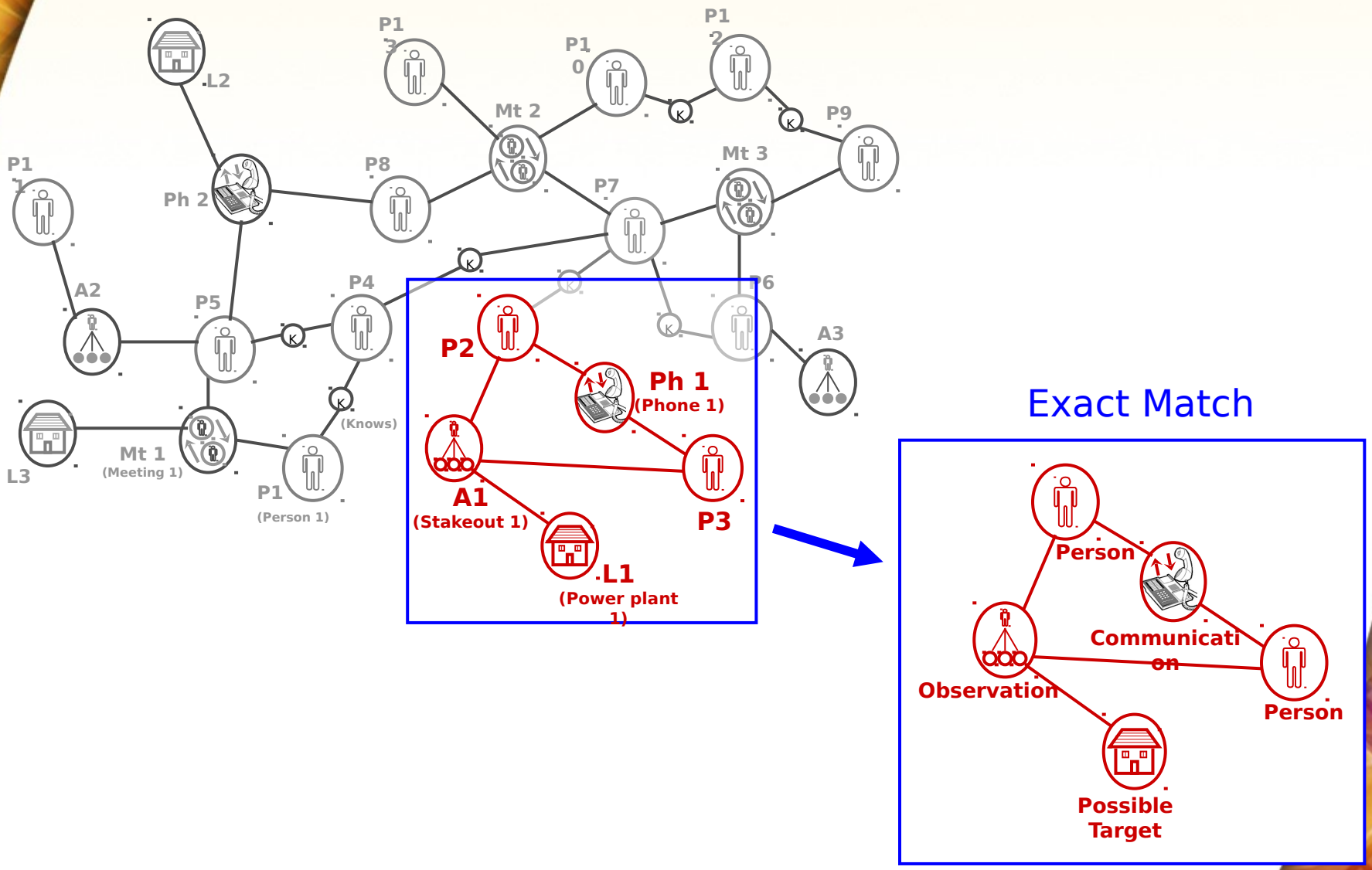


Sample Input Graph (Ground Truth / Observations)

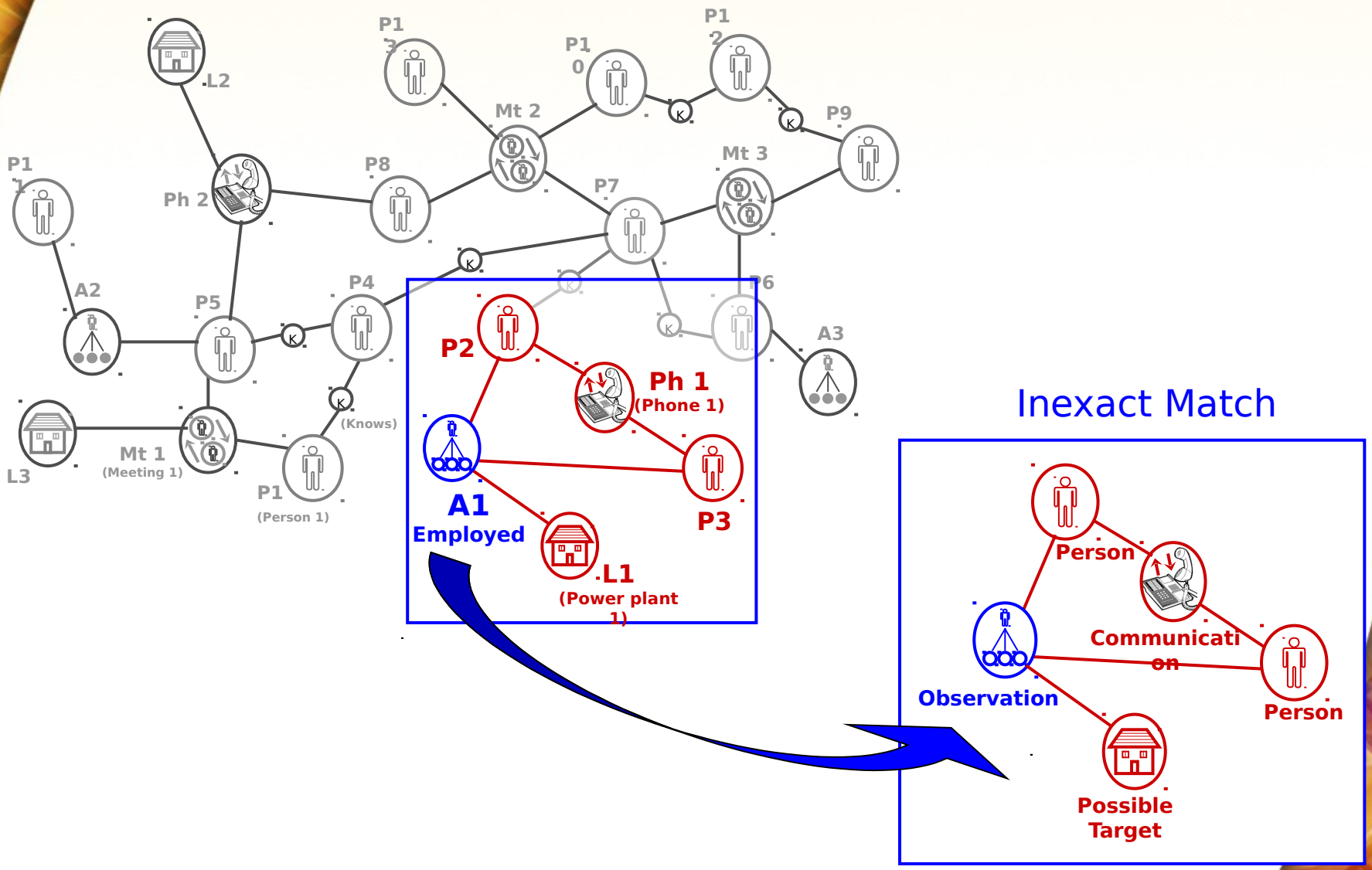




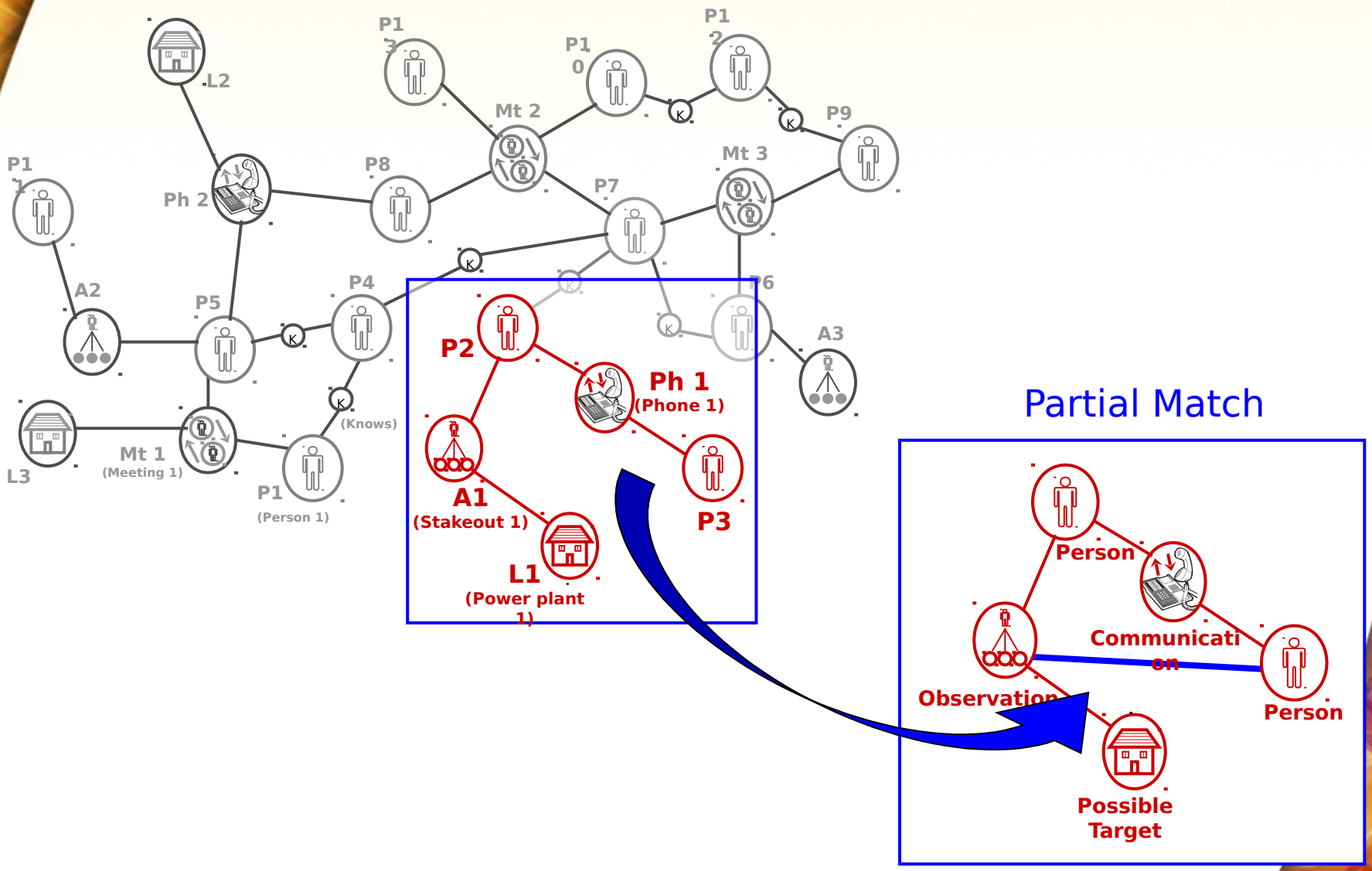
Exact Pattern Matching



Inexact Matching



Partial Matching

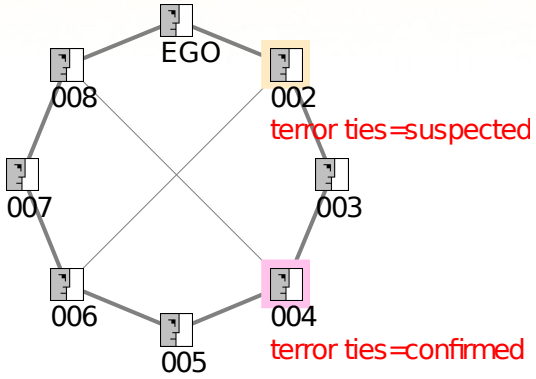


Approach Overview – Social Network Analysis

- Social network analysis metrics quantify different aspects of an activity or communication graph's topology
- Social network analysis signatures define how to classify groups in terms of their SNA metric values
  - Classifications: What conclusions the search can reach
  - Features: SNA metrics used to classify groups
  - Decision Rules: Mapping between feature values and classifications
- Novel suspicious activity is classified based on signatures that capture
  - Expert knowledge
  - Statistical similarity to previous suspicious activity

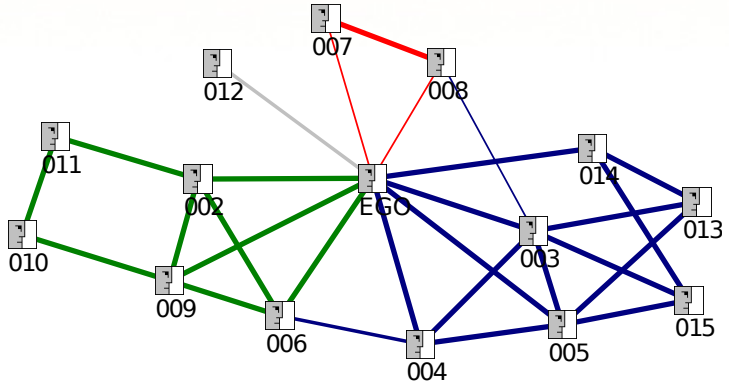
Normal vs. Abnormal Social Network Patterns

ABNORMAL



- Only one type of cluster
- Density too low
- No family links
- No links outside of this group
  - look for 2nd and 3rd step links out from this group!
- More distant links than local links
- Social network looks 'man-made' i.e. like a computer network

NORMAL

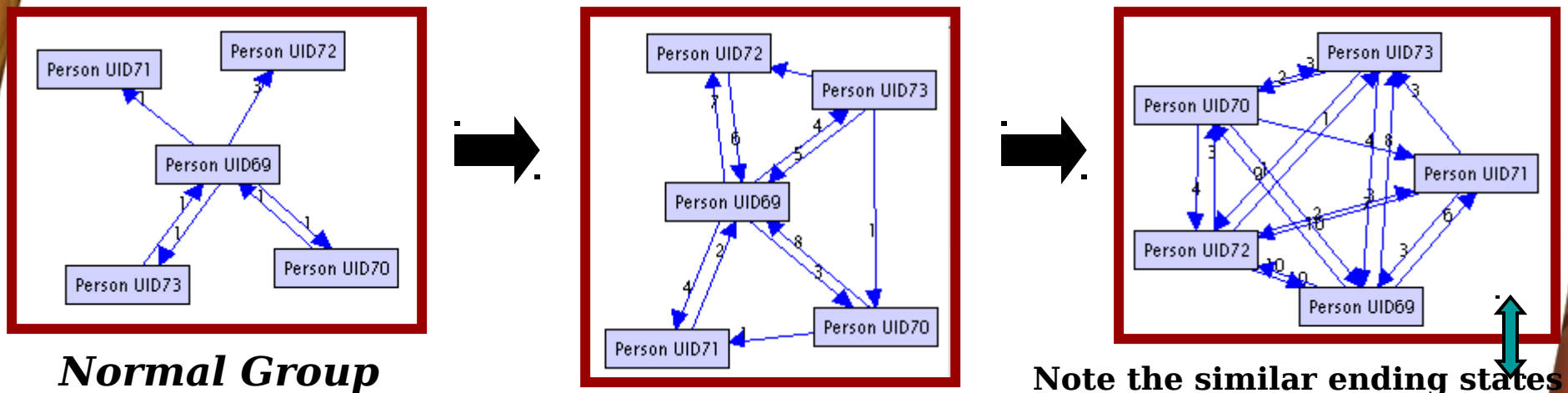


- Distinct clusters
  - Red = family
    Blue = work
    Green = friends.
- Closed Trios
  - If Mary knows Alice and Alice knows John, then Mary knows John.
- More local than distant links

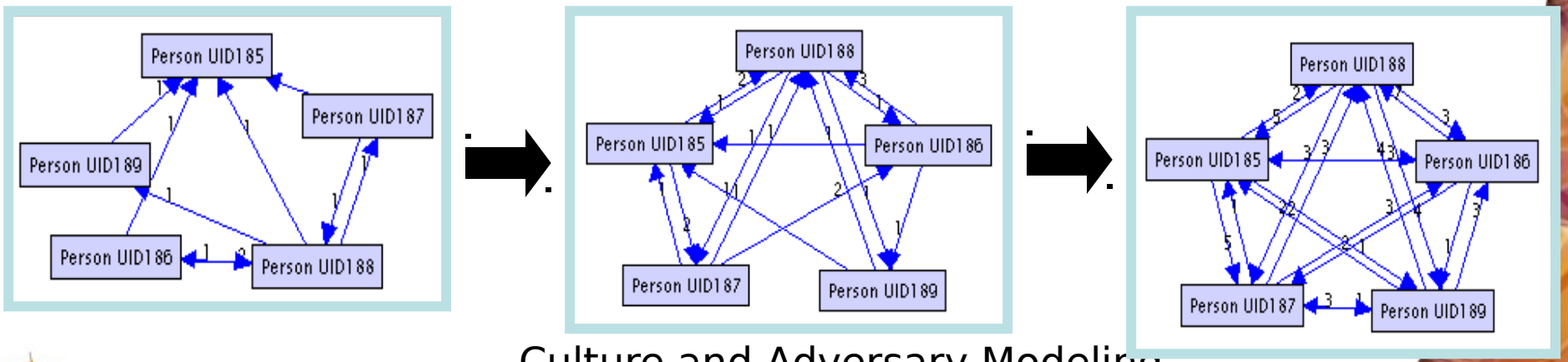
Dynamic Social Network Analysis Metrics

- Some groups are anomalous not because of how they look at some moment in time, but because of how they *evolve*

Activating Cell

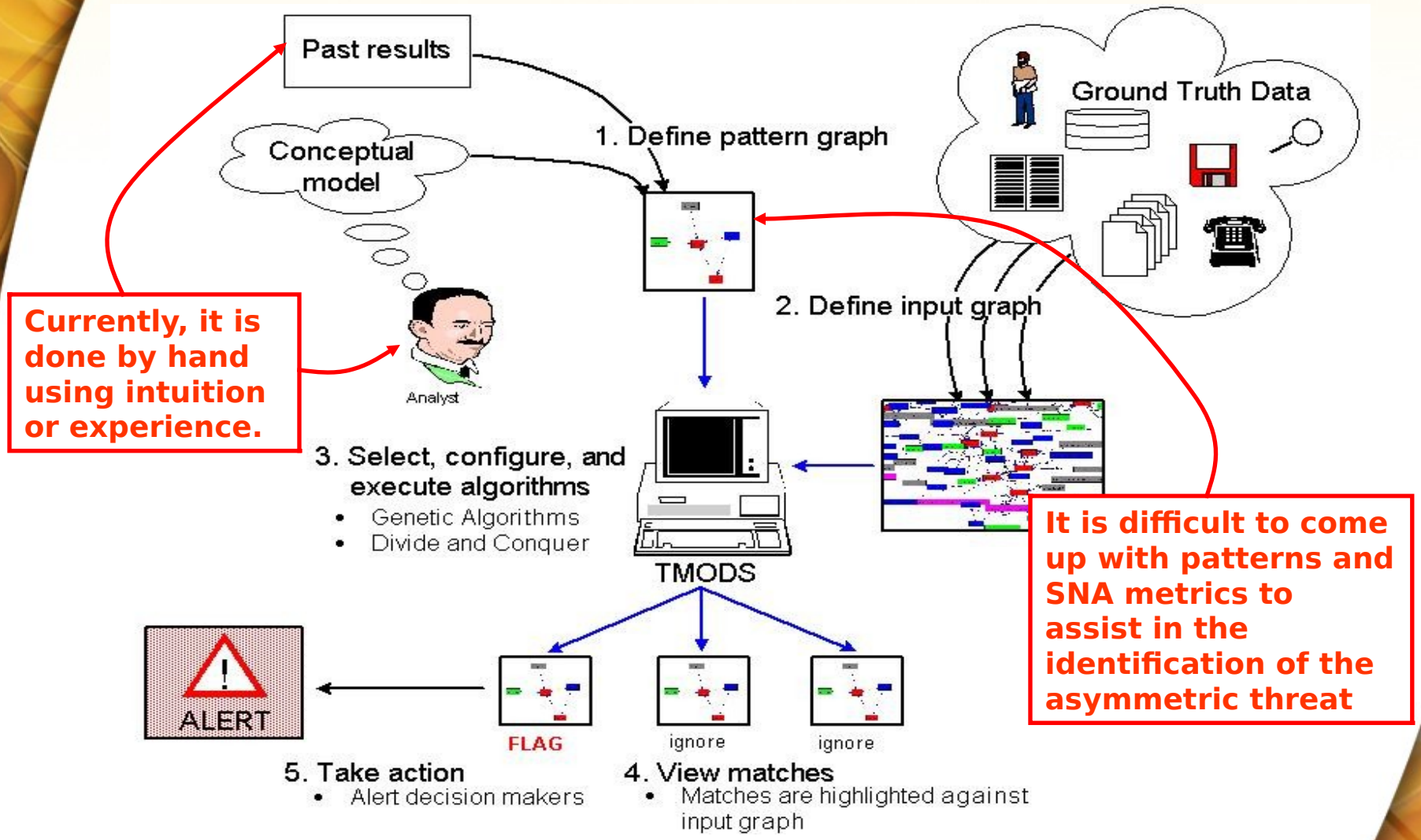


Normal Group

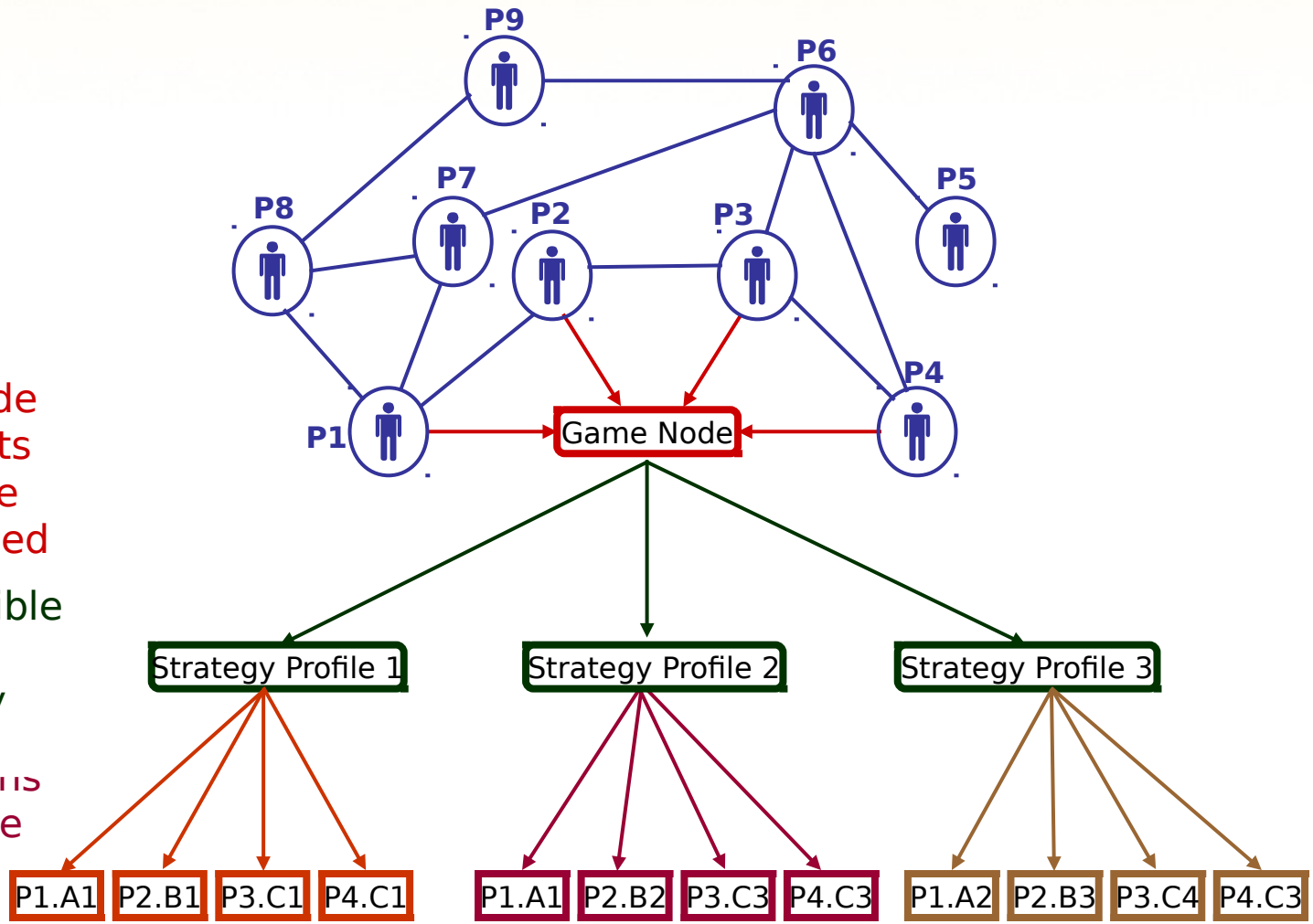


Note the similar ending states

GT-TMODS – Concept of Operations


Past results
Conceptual model
1. Define pattern graph
Ground Truth Data
Currently, it is done by hand using intuition or experience.
Analyst
2. Define input graph
3. Select, configure, and execute algorithms
• Genetic Algorithms
• Divide and Conquer
TMODS
It is difficult to come up with patterns and SNA metrics to assist in the identification of the asymmetric threat
ALERT
FLAG
ignore
ignore
5. Take action
• Alert decision makers
4. View matches
• Matches are highlighted against input graph

Game Representation in TMODS



Game Node Represents the Game Being Played

Three Possible Stable Strategy Profiles

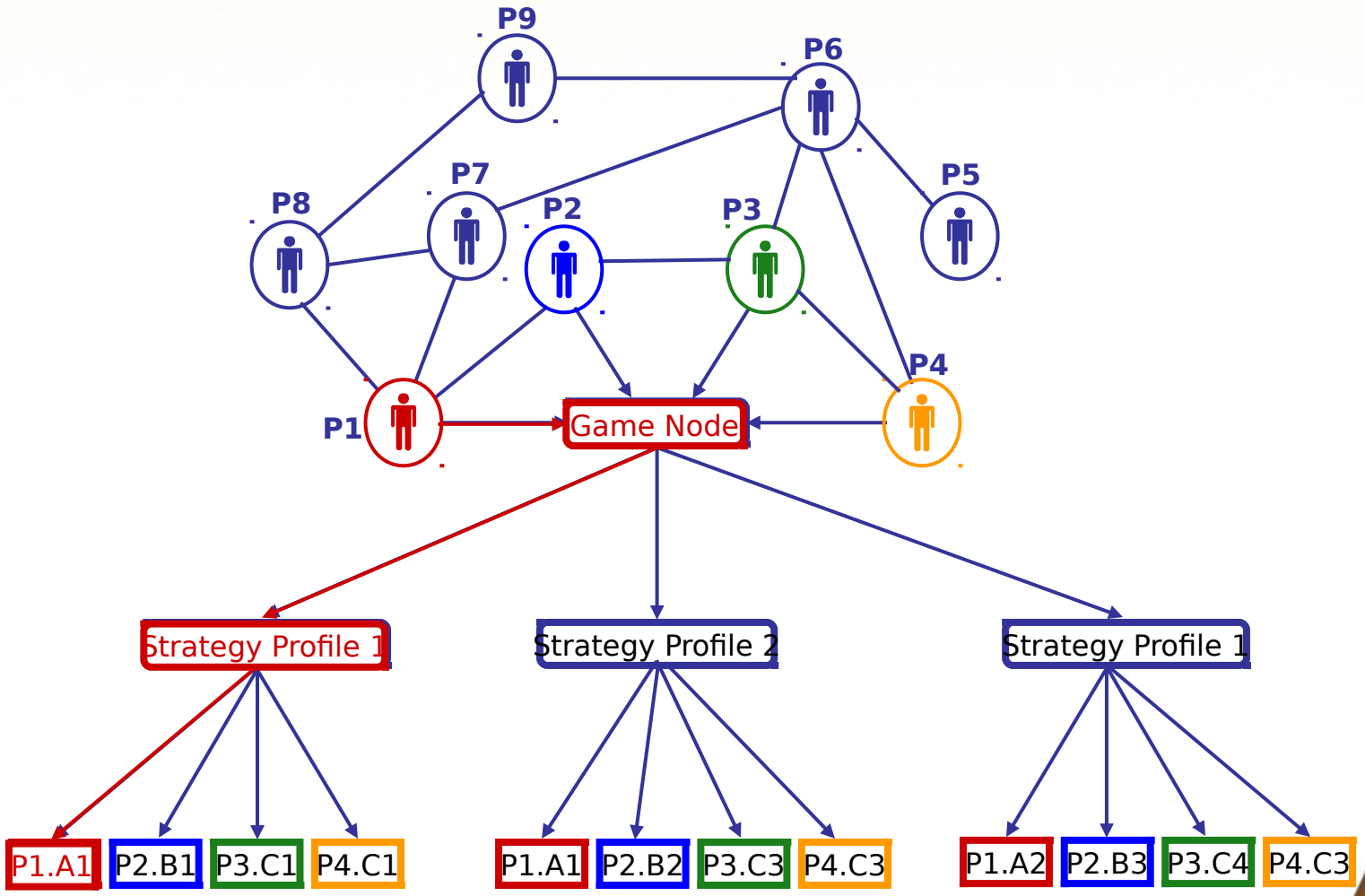
Four actions per profile

Pattern Matching Scenario

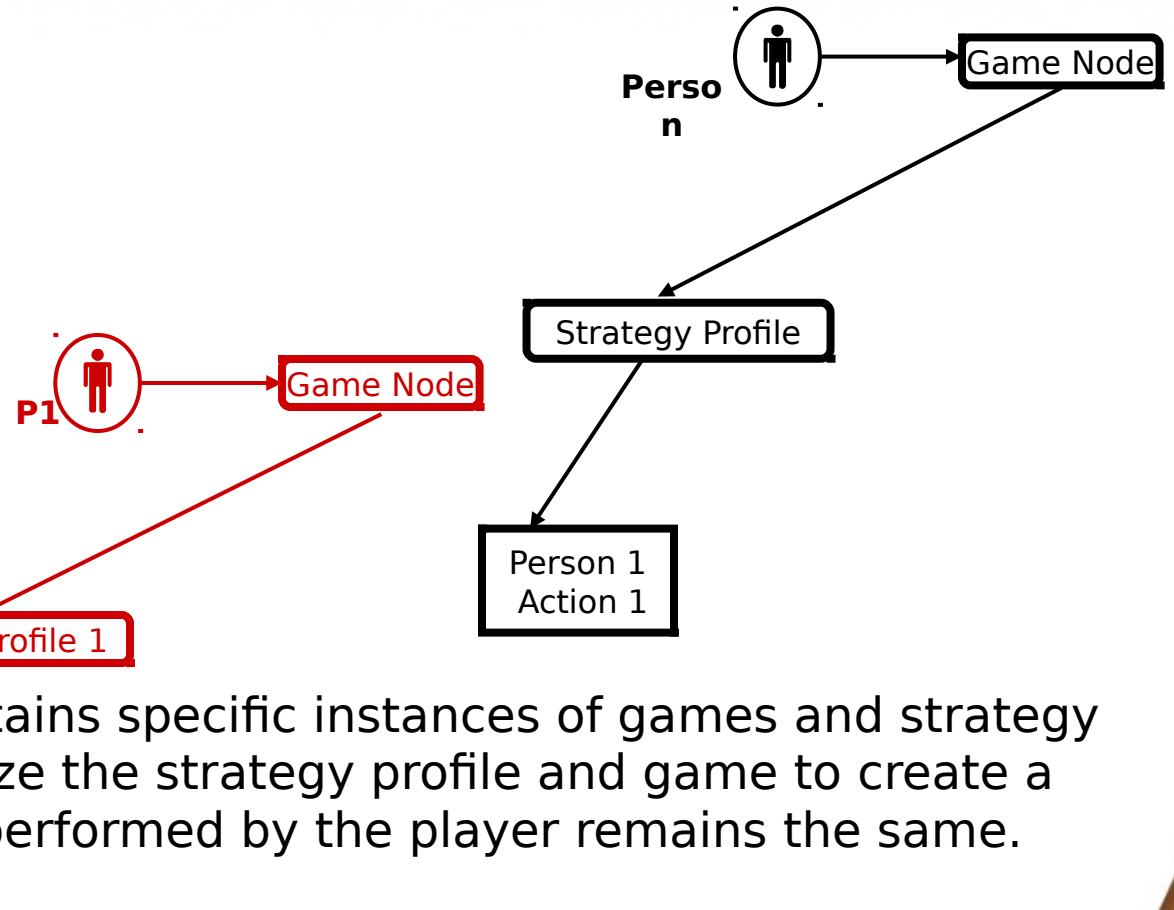
- Suppose we know that some group of players are collaborating, and this collaboration is modeled as a game.
- We don’t know what possible strategies are in play.
  - We know the possibilities
- How can we leverage pattern matching and game-theoretic modeling to predict future actions?
  - Model observed actions as a pattern
    - We know that P1 has performed A1
    - What can this tell us about the actions of other players?

Pattern Matching Scenario

Each *Player (P#)* is associated with an *Action (A#)* for each *Strategy (Strat #)*



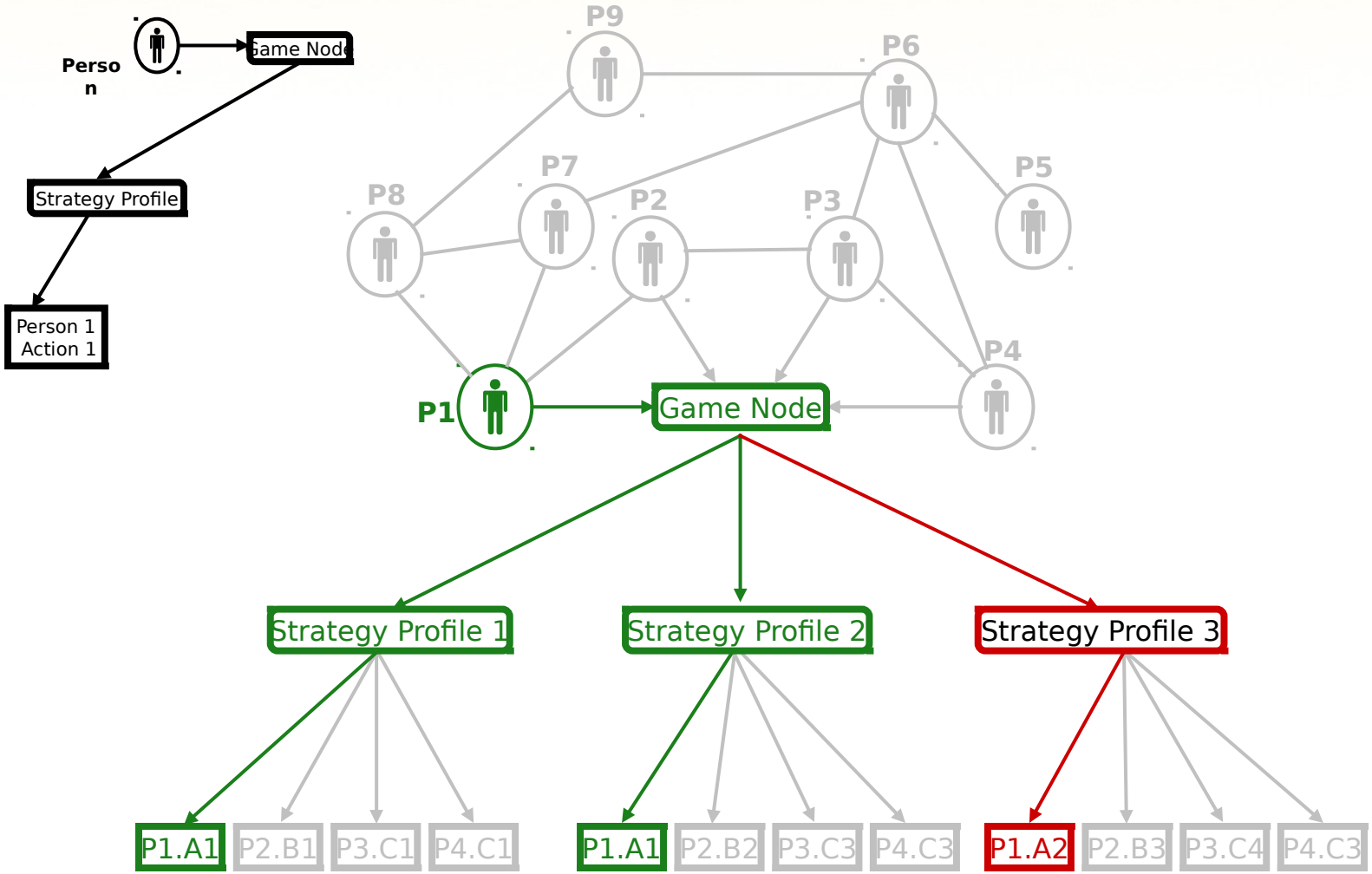
Pattern Matching Scenario



The input graph contains specific instances of games and strategy profiles. We generalize the strategy profile and game to create a pattern. The action performed by the player remains the same.

Pattern Matching Scenario

Game Theory TMODS uses these associations to detect possible threat patterns.

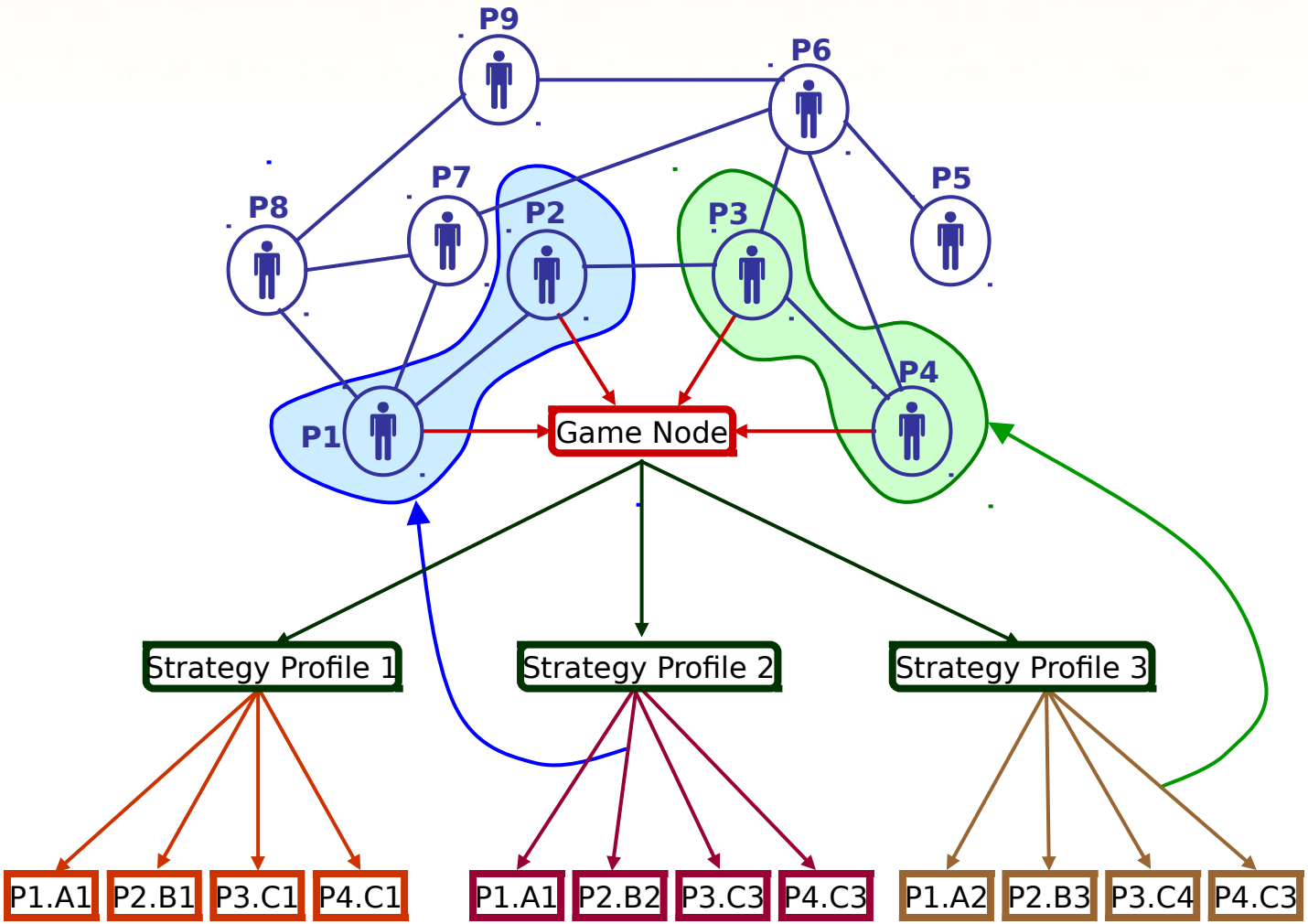


Group (Coalition) Detection Scenario

- 21st Century has developed a SNA-based group detection algorithm based on someone's network of "best friends."
  - A person's network of friends tend to know each other.
- UM has developed a coalition detection algorithm using game theoretic methods
  - Given a payoff matrix, what are the probabilities that various coalitions will form to maximize the joint payoff?
- How can these group detection methods be fused to provide higher-level situational awareness?

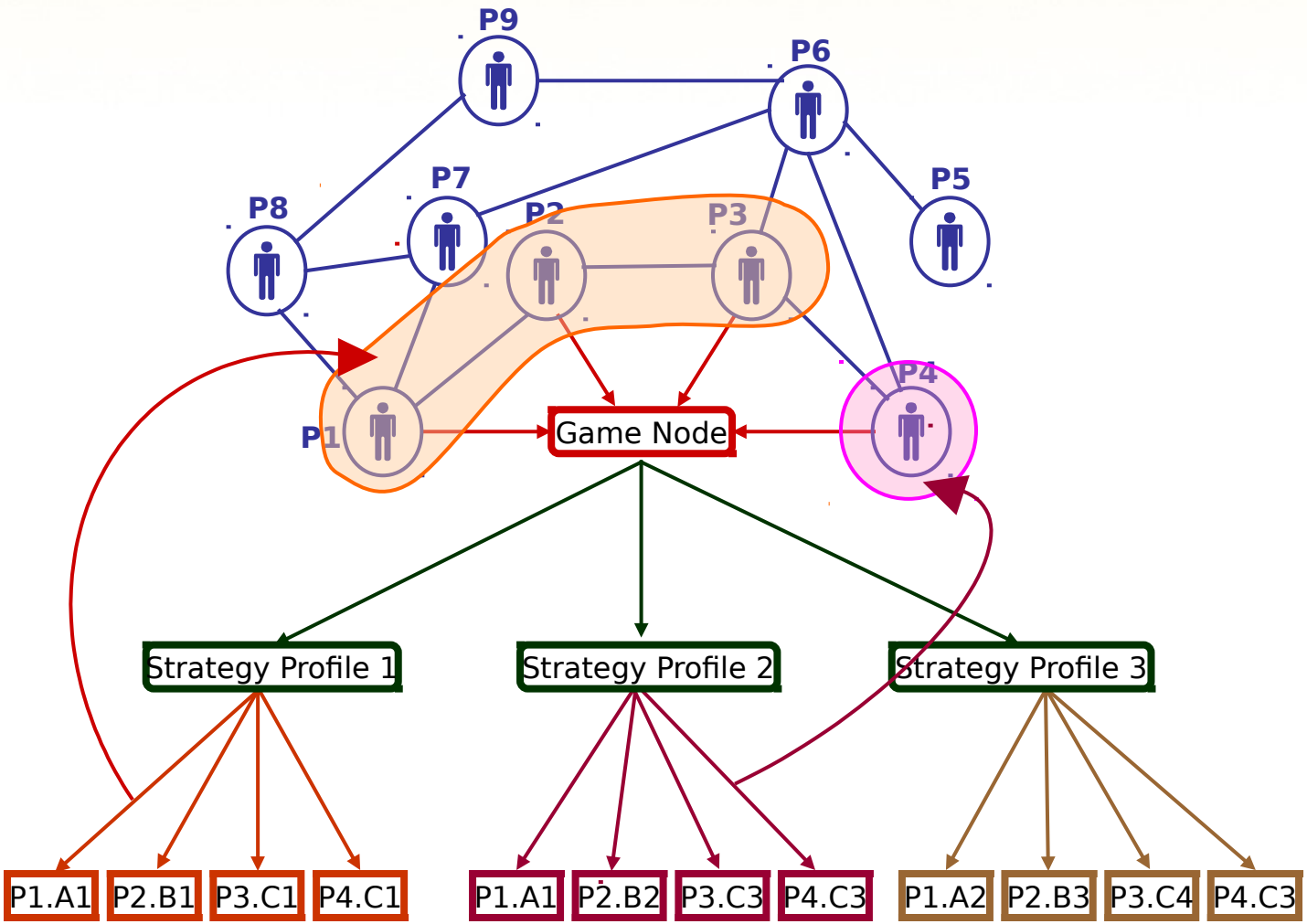
Group (Coalition) Detection Scenario

Groups Detected by Game Theory



Group (Coalition) Detection Scenario

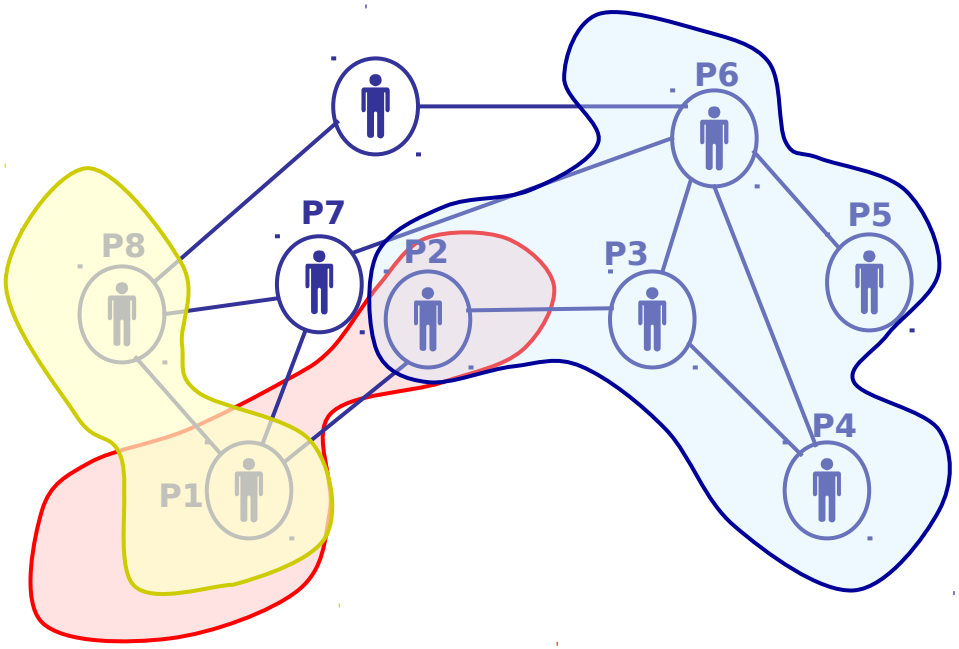
Groups Detected by Game Theory



Group (Coalition) Detection Scenario

Group Detection via SNA

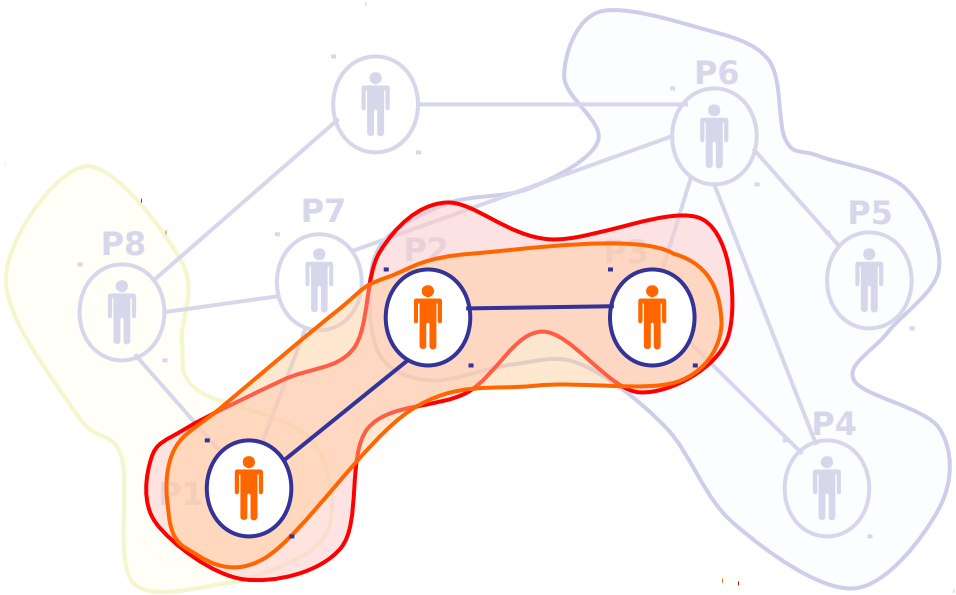
Groups Detected by Social Network Analysis



Group (Coalition) Detection Scenario

SNA Groups Compared to GT Groups

By laying SNA Groups on top of GT Groups.



GT-TMODS Contributions

- Use game-theory to model and derive graph patterns
  - Analytic and simulated solutions to multi-player games
  - TMODS can search over large datasets of instances of a game
- Use game-theory to model and derive social networking relationships
  - Coalitions, cut-outs
  - The network of games may reveal social networking relationships (probabilistic)
  - Conversely, the existence of known social networking relationships may reveal the likely games in play, or the payoffs of individuals
- We are *not* modeling new game types, not are we finding new methods to solve games.
  - We integrate game-theory results into our graph pattern matching and SNA framework.

Key Ideas

- Game-theoretic methods will be used to infer player actions, given a description of the game.
- Special “game node” will be used to represent the description of the game.
  - Initially, normal form games (payoff matrices)
- TMODS pattern matching algorithm will be extended to ***augment*** the graph by adding action nodes and coalition nodes resulting from solutions to a game.
  - Once actions and coalitions are added, traditional TMODS pattern matching and SNA algorithms can be used
- Algorithm will be tested by generating synthetic graphs, using Gamut and other tools for game generation.

Questions?

- Contact Information

Tim Darr, Ph.D. (tdarr@21technologies.com)
Technical Team Lead
21st Century Technologies (www.21technologies.com)